Introduction

Savings associations, along with other types of financial institutions, are developing and employing new electronic technologies for delivering financial products to improve customer service and lower costs. The new technologies being offered include on-line financial services, stored value card systems, and electronic cash. Services and products can be accessed through personal computers connecting to participating institutions via proprietary software, commercial on-line services, and the Internet, or through other access devices including, for example, video kiosks and interactive television. The most significant growth involves the establishment of Internet web sites by institutions that are used to advertise products and services, accept electronic mail, and provide consumers with the capability to conduct transactions through an on-line system.

The regulatory environment continues to evolve in response to the introduction and implementation of new electronic banking technologies. However, it is important to keep in mind that the new technologies merely offer an alternative means for delivering traditional products and services; they do not represent new or different banking products standing alone. Existing consumer laws and regulations generally apply to transactions, advertisements and other services conducted electronically. This Section is intended to describe how existing compliance rules are applied to the emerging electronic banking technologies. Additionally, this Section highlights new developments in compliance intended to address some of the unique aspects of the new electronic services. References to applicable consumer affairs, compliance, and fair lending laws and regulations are made in the various policy statements, guidance, proposed rule changes, and reports discussed or included herein.

Regulatory Guidance

Some recent guidance has been issued to address consumer compliance concerns arising from use of the new technologies:

Interagency Guidance on Electronic Financial Services and Consumer Compliance, issued by the FFIEC in July 1998 (soon to be reissued with updated information).

Policy Statement on Privacy and Accuracy of Personal Customer *Information* and *Interagency Pretext Phone Calling Memorandum*, both issued by OTS in November 1998

The interagency guidance is intended to assess the implications of some of the emerging electronic technologies for the consumer regulatory environment, to provide institutions with an overview of pertinent regulatory issues, and to offer suggestions on how to apply existing consumer laws and regulations to new electronic financial services. It also seeks to promote compliance with relevant laws and regulations. The guidance contains two sections, one on the compliance regulatory environment and the other on the role of consumer compliance in developing and implementing electronic services. The text of the document is included in full within this section.

The policy statement and pretext phone calling memorandum are intended to enhance awareness of customer privacy. They reflect the OTS' understanding of certain "best practices" that may help to adequately protect personal information. Please note, however, that Sections 501(b) and 502 of GLBA supersede the policy statement to a significant degree, although some of the best practice elements remain relevant and worthy of consideration. Both the policy statement and the memorandum are included in this section following the interagency guidance.

Electronic Delivery of Consumer Disclosures: Recent Developments

The Federal Reserve Board of Governors (the Board) issued two "Interim Final" Rules, in early 2001, on the electronic delivery of consumer disclosures required under Regulations B, D, E, M and Z. With the Rules, the Board sought to establish uniform standards for institutions offering fi-

nancial products and services to its customers in an electronic environment. The Board established October 1, 2001 as the mandatory compliance date, but continued to seek additional public comment in the period following the issuance of the Interim Final Rules.

The Interim Final Rules provide guidance on the timing and delivery of electronic disclosures. Disclosures can be provided by e-mail or can be made available at another location such as an institution's web site. If a disclosure - such as an account statement or a notice of change in account terms - is provided at a web site, an institution must notify the consumer of the disclosure's availability by e-mail. In addition, the disclosure must remain available on the web site for 90 days.

A number of commenters noted various discordant issues posed by the Interim Final rules and the Electronic Signatures in Global and National Commerce Act (the E-Sign Act), enacted in June 2000 and effective October 1, 2000. Section 101 of the E-Sign Act provides that information required by law to be in writing can be made available electronically to a consumer only if he or she affirmatively consents to receive the information electronically and the business clearly and conspicuously discloses specified information to the consumer before obtaining his or her consent. Although both the Interim Final Rules and the E-Sign Act address appropriate disclosure measures, the standards for compliance are not the same.

Other commenters to the Board's Rules requested more time to address technology modifications and to review existing policies and practices in light of the proposed regulatory requirements. Thus, on August 3, 2001, the Board announced that it is considering adjustments to the rules to provide additional flexibility, based on the commenters' concerns. The Board also lifted the mandatory compliance date of October 1, 2001 and directed institutions to follow their existing procedures[1] or, alternatively, to comply with the Interim Final Rules until permanent rules are issued. Once permanent final rules are issued, the Board expects to afford institutions a reasonable period of time to comply with those rules.

The complete text of the Interim Final Rules can be found at:

66 FR 17779 (Regulation B, Equal Credit Opportunity)

66 FR 17786 (Regulation E, Electronic Fund Transfers)

66 FR 17322 (Regulation M, Consumer Leasing)

66 FR 17329 (Regulation Z, Truth in Lending)

66 FR 17795 (Regulation DD, Truth in Savings)

The complete text of section 101(c) of the E-Sign Act can be found at:

http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ229.106.pdf

For further information, consult the Federal Reserve Board's website at:

http://www.bog.frb.fed.us

Consumer Electronic Payments Task Force

The Consumer Electronic Payments Task Force was comprised of the four bank regulatory agencies together with the Financial Management Service, the Federal Reserve Bank of Atlanta, and the Federal Trade Commission. The Task Force, with the participation of the industry and the public, attempted to: (1) identify the primary consumer issues arising from electronic money products, (2) evaluate the extent to which the issues are addressed by state and federal laws and regulations and voluntary industry guidelines, and (3) identify nonregulatory responses to address the remaining issues. The final report is divided into four areas of consumer concern: Access, Privacy, Financial Condition of Issuers, and Consumer Disclosures and Protections.

[1] Presumably, existing procedures of the institution are compliant with earlier Federal Reserve interim rules issued in 1998 and 1999 in addressing Regulations E and DD, respectively; or compliant with the E-Sign Act (effective as of October 1, 2000) in addressing Regulations B, M and Z.

The Task Force report did not recommend any governmental regulatory responses at time of its issuance (April 1998), but did recommend that the industry develop effective self-regulatory techniques to address consumer concerns. The final report did include recommendations on the role of government in providing consumer financial education, monitor industry developments, and encourage appropriate industry action. It also contains specific recommended actions on each of the four areas that should be taken by the industry.

The final report and other related information can be found at the web site of the Office of the Comptroller of the Currency located at www.occ.treas.gov.

Examination Procedures

Currently, the only examination procedures specific to electronic banking are included in this section as Appendix D, which addresses the Children's Online Privacy Protection Act. Over time, the four bank regulatory agencies intend to insert pertinent revisions into existing examination procedures that take into account use of the new electronic technologies by financial institutions. Rather than developing a single set of examination procedures relating to all aspects of electronic banking, the agencies intend to respond to new statutes and regulations while making changes to existing examination procedures for consumer affairs and compliance laws and regulations as they are identified.

Interagency Guidance on Electronic Financial Services and Consumer Compliance
See Appendix A.

Policy Statement on Privacy and Accuracy of Personal Customer
See Appendix B.

Interagency Pretext Phone Calling Memorandum
See Appendix C.

Children's Online Privacy Protection Act
See Appendix D.

FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL

INTERAGENCY GUIDANCE ON ELECTRONIC FINANCIAL SERVICES AND CONSUMER COMPLIANCE[1]

INTRODUCTION

Federally insured depository institutions are developing or employing new electronic technologies for delivering financial products to improve customer service and enhance competitive positions. Some of those institutions have asked regulators questions regarding the application of existing consumer protection laws and regulations to electronic product delivery methods. It is clear from these questions that these institutions are uncertain about the appropriate manner to address electronic services under the existing regulatory framework. Accordingly, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision (collectively, the "Agencies") are providing federally insured depository institutions with some basic information and suggested guidance pertaining to federal consumer protection laws and regulations and their application to electronic financial service operations.

This issuance is intended to assess the implications of some of the emerging electronic technologies for the consumer regulatory environment, to provide institutions with an overview of pertinent regulatory issues, and to offer suggestions on how to apply existing consumer laws and regulations to new electronic financial services.

The term "electronic financial service" as used in this guidance includes, but is not limited to, on-line financial services, electronic fund transfers, and other electronic payment systems. On-line financial services, stored value card systems, and electronic cash are among the new electronic products being introduced in the market. Financial institutions are establishing Internet web sites that advertise products and services, accept electronic mail, and provide consumers with the capability to conduct transactions through an on-line system. Services and products can be accessed through personal computers connecting to the institution via proprietary software, commercial on-line services, and the Internet, or through other access devices including, for example, video kiosks and interactive television. Financial institutions should be advised that many of the general principles, requirements, and controls that apply to paper transactions may also apply to electronic financial services. This guidance letter contains two sections: 1) The Compliance Regulatory Environment, and 2) The Role of Consumer Compliance in Developing and Implementing Electronic Services. Examples relating to compliance issues are used for illustrative purposes; institutions are encouraged to use the concepts underlying these examples when implementing an electronic services technology plan. It should be understood that existing consumer laws and regulations generally apply to applicable transactions, advertisements and other services conducted electronically. It should also be understood, however, that not all of the consumer protection issues that have arisen in

[1] This document does not serve as an Official Staff Commentary or shield institutions that comply with this guidance from civil liability for violations under the various statutes addressed.

connection with new technologies are specifically addressed in this guidance. Additional communiqués may be issued in the future to address other aspects of consumer laws and regulations as the financial service environment evolves.

COMPLIANCE REGULATORY ENVIRONMENT

This section summarizes and highlights the most recent changes in the relevant sections of federal consumer protection laws and regulations that address electronic financial services, and notes other relevant provisions of law. This information is not intended to be a complete checklist for consumer compliance in the electronic medium. It does not address a number of open issues surrounding the application of consumer rules to new electronic financial services that are currently being considered by the appropriate agencies. It is critical that institutions providing electronic delivery mechanisms develop and maintain an in-depth knowledge of the relevant statutes and regulations. Moreover, it should be kept in mind that additional changes to relevant laws and regulations arising in response to the new electronic service technologies may occur. The rapid development of technology and new products will require updating of this information.

Generally, the regulatory requirement that disclosures be in writing and in a form the customer can keep has been met by providing paper disclosures to the customer. For example, a bank would supplement electronic disclosures with paper disclosures until the regulations have been reviewed and changed, if necessary, to specifically allow electronic delivery of disclosures. Some of the consumer regulations were reviewed and changed to reflect electronic disclosures. These changes are summarized in this section. Also, attached to this guidance is a matrix entitled "Compliance Issues Involving Electronic Services" that highlights some of the principal compliance issues that should be considered by financial institutions when developing and implementing electronic systems.

DEPOSIT SERVICES

Electronic Fund Transfer Act (Regulation E)

Generally, when on-line banking systems include electronic fund transfers that debit or credit a consumer's account, the requirements of the Electronic Fund Transfer Act and Regulation E apply. A transaction involving stored value products is covered by Regulation E when the transaction accesses a consumer's account (such as when value is "loaded" onto thecard from the consumer's deposit account at an electronic terminal or personal computer).

In accordance with §205.4, financial institutions must provide disclosures that are clear and readily understandable, in writing, and in a form the consumer may keep. An Interim rule was issued on March 20, 1998 that allows depository institutions to satisfy the requirement to deliver by electronic communication any of these disclosures and other information required by the act and regulations, as long as the consumer agrees to such method of delivery. According to the Federal Reserve Board Official Staff Commentary (OK) §205.7(a)-4, financial institutions must ensure that consumers who sign-up for a new banking service are provided with disclosures for the new service if the service is subject to terms and conditions different from those described in the initial disclosures required under §205.7. Although not specifically mentioned in the commentary, this applies to all new banking services including electronic financial services.

The OSC also clarifies that terminal receipts are unnecessary for transfers initiated on-line. Specifically, OSC 4205.2(h)-1 provides that, because the term "electronic terminal" excludes a telephone operated by a consumer, financial institutions need not provide a terminal receipt when a consumer initiates a transfer by a means analogous in function to a telephone, such as by a personal computer or a facsimile machine.

Additionally, OSC §205.10(b)-5 clarifies that a written authorization for preauthorized transfers from a consumer's account includes an electronic authorization that is not signed, but similarly authenticated by the consumer, such as through the use of a security code. According to the OSC, an example of a consumer's authorization that is not in the form of a signed writing but is, instead, "similarly authenticated" is a consumer's authorization via a home banking system. To satisfy the regulatory requirements, the institution must have some means to identify the consumer (such as a security code) and make a paper copy of the authorization available (automatically or upon request). The text of the electronic authorization must be displayed on a computer screen or other visual display that enables the consumer to read the communication from the institution. Only the consumer may authorize the transfer and not, for example, a third-party merchant on behalf of the consumer.

Pursuant to §205.6, timing in reporting an unauthorized transaction, loss, or theft of an access device determines a consumer's liability. A financial institution may receive correspondence through an electronic medium concerning an unauthorized transaction, loss, or theft of an access device. Therefore, the institution should ensure that controls are in place to review these notifications and also to ensure that an investigation is initiated as required.

Truth in Savings Act (Regulation DD)

Financial institutions that advertise deposit products and services on-line must verify that advertising disclosures are made in accordance with all provisions of §230.8. Institutions should note that the disclosure exemption for electronic media under §230.8(e) does not specifically address commercial messages made through an institution's web site or other on-line banking system. Accordingly, adherence to all of the advertising disclosure requirements of §230.8 is required.

Advertisements should be monitored for recency, accuracy, and compliance. Financial institutions should also refer to OSC §230.2(b)-2(i) if the institution's deposit rates appear on third party web sites or as part of a rate sheet summary. These types of messages are not considered advertisements unless the depository institution, or a deposit broker offering accounts at the institution, pays a fee for or otherwise controls the publication.

Pursuant to §230.3(a), disclosures generally are required to be in writing and in a form that the consumer can keep. Until the regulation has been reviewed and changed, if necessary, to allow electronic delivery of disclosures, an institution that wishes to deliver disclosures electronically to consumers, would supplement electronic disclosures with paper disclosures.

Expedited Funds Availability Act (Regulation CC)

Generally, the rules pertaining to the duty of an institution to make deposited funds available for withdrawal apply in the electronic financial services environment. This includes rules on fund availability schedules, disclosure of policy, and payment of interest. Recently, the FRB published a commentary that clarifies requirements for providing certain written notices or disclosures to customers via electronic means. Specifically, the commentary to §229.13(g)-la states that a financial institution satisfies the written exception hold notice requirement, and the commentary to §229.15(a)-1 states that a financial institution satisfies the general disclosure requirement by sending an electronic version that displays the text and is in a form that the customer may keep. However, the customer must agree to such means of delivery of notices and disclosures. Information is considered to be in a form that the customer may keep if, for example, it can be downloaded or printed by the customer. To reduce compliance risk, financial institutions should test their programs' ability to provide disclosures in a form that can be downloaded or printed.

Reserve Requirements of Depository institutions (Regulation D)

Pursuant to the withdrawal and transfer restrictions imposed on savings deposits §204.2(d)(2) electronic transfers, electronic withdrawals (paid electronically) or payments to third parties initiated by a depositor from a personal computer are included as a type of transfer subject to the six transaction limit imposed on passbook savings and MMDA accounts.

Institutions also should note that, to the extent stored value or other electronic money represents a demand deposit or transaction account, the provisions of Regulation D would apply to such obligations.

LOAN/LEASING SERVICES

Truth in Lending Act (Regulation Z)

The commentary to regulation Z was amended recently to clarify that periodic statements for open-end credit accounts may be provided electronically, for example, via remote access devices. OSC §226S(b)(2)(ii)-3 states that financial institutions may permit customers to call for their periodic statements, but may not require them to do so. If the customer wishes to pick up the statement and the plan has a grace period for payment without imposition of finance charges, the statement, including a statement provided by electronic means, must be made available in accordance with the "14-day rule," requiring mailing or delivery of the statement not later than 14 days before the end of the grace period.

Provisions pertaining to advertising of credit products should be carefully applied to an on-line system to ensure compliance with the regulation. Financial institutions advertising open-end or closed-end credit products on-line have options. Financial institutions should ensure that on-line advertising complies with §226.16 and §226.24.. For on-line advertisements that may be deemed to contain more than a single page, financial institutions should comply with §226.16(c) and §226.24(d), which describe the requirements for multiple-page advertisements.

Consumer Leasing Act (Regulation M)

OSC §213.2(b)-1 provides examples of advertisements that clarity the definition of an advertisement under Regulation M. The term advertisement includes messages inviting, offering, or otherwise generally announcing to prospective customers the availability of consumer leases, whether in visual, oral, print, or electronic media. Included in the examples are on-line messages, such as those on the Internet. Therefore, such messages are subject to the general advertising requirements under §213.7.

Equal Credit Opportunity Act (Regulation B)

OSC §2025(e)-3 clarifies the rules concerning the taking of credit applications by specifying that application information entered directly into and retained by a computerized system qualifies as a written application under this section. If an institution makes credit application forms available through its on-line system, it must ensure that the forms satisfy the requirements of §202.5.

OSC §202.13(b)-4 also clarifies the regulatory requirements that apply when an institution takes loan applications through electronic media. If an applicant applies through an electronic medium (for example, the Internet or a facsimile) without video capability that allows employees of the institution to see the applicant, the institution may treat the application as if it were received by mail.

FAIR HOUSING ACT

A financial institution that advertises on-line credit products that are subject to the Fair Housing Act must display the Equal Housing Lender logotype and legend or other permissible disclosure of its nondiscrimination policy if required by rules of the institution's regulator (OTS §528.4, FDIC 9338.3, NCUA §701.31, FRB Fair Housing Advertising and Poster Requirements, 54 Fed. Reg. 11,567 (1989)).

HOME MORTGAGE DISCLOSURE ACT (REGULATION C)

OSC §203.4(a)(7)-5 clarifies that applications accepted through electronic media with a video component (the financial institution has the ability to see the applicant) must be treated as "in person" applications. Accordingly, information about these applicants' race or national origin and sex must be collected. An institution that accepts applications through electronic media without a video component, for example, the Internet or facsimile, may treat the applications as received by mail.

FAIR CREDIT REPORTING ACT

The Economic Growth and Regulatory Paperwork Reduction Act of 1996 (Public Law 104-208, §2408, 110 Stat. 3009 (1996)) amended Section 610 of the Fair Credit Reporting Act (15 U.S.C. 5 168 1 h), to allow consumer reporting agencies to make the disclosures to consumers required under Section 609 by electronic means if authorized by the consumer. Consumers must specify that they wish to receive the disclosures in an electronic form, and such form of delivery must be available from the credit reporting agency.

Any participant in an electronic service system who regularly gathers or evaluates consumer credit information or other information about consumers for the purpose of furnishing consumer reports to third parties (for monetary fees, dues, or on a cooperative nonprofit basis) is considered a consumer reporting agency. In such cases, the participant must comply with the applicable provisions of the FCRA.

MISCELLANEOUS

ADVERTISEMENT OF MEMBERSHIP (FDIC 12CFR 5328) (NCUA RR 740)

The FDIC and NCUA consider every insured depository institution's on-line system top level page, or "home page", to be an advertisement. Therefore, according to these agencies' interpretation of their rules, financial institutions subject to §328.3 (NCUA RR 9740.4) should display the official advertising statement on their home pages unless subject to one of the exceptions described under 5328.3(c) (NCUA RR9740.4(c)). Furthermore, each subsidiary page of an on-line system that contains an advertisement should display the official advertising statement unless subject to one of the exceptions described under §328.3(c) (NCUA RR4740.4(c)). Additional information about the FDIC's interpretation can be found in the Federal Register, Volume 62, page 6145, dated February 11, 1997.

The official bank sign (FDIC §328.2), official savings association sign (FDIC §328.4), and NCUA official sign (NCUA RR 740.3) are currently not required to be displayed on an institution's on-line system.

FAIR DEBT COLLECTION PRACTICES ACT

According to Section 803(2) of the Fair Debt Collection Practices Act (15 U.S.C. 9 1692a(2)), "communication" means conveying information regarding a debt directly or indirectly to any person through any medium. Financial institutions acting as debt collectors for third parties are permitted to communicate via electronic means, such as the Internet, to collect a debt or to obtain information about a consumer. In such instances, financial institutions must ensure that their communications and practices are in keeping with the requirements of the Act.

FLOOD DISASTER PROTECTION ACT

The regulation implementing the National Flood Insurance Program requires a financial institution to notify a prospective borrower and the servicer that the structure securing the loan is located or to be located in a special flood hazard area. The regulation also requires a notice of the servicer's identity be delivered to the insurance provider. While the regulation addresses electronic delivery to the servicer and to the insurance provider, it does not address electronic delivery of the notice to the borrower.

COMPLIANCE POLICY GUIDANCE

The following discussion provides specific interim compliance policy guidance regarding advertising, disclosures/notices, applications, stored value cards, and record keeping. This guidance is intended to discuss the regulations' requirements as presently written in the context of the electronic financial services environment and, to the extent possible, to provide practical examples for application of this guidance. This guidance may have to be reconsidered and revised at such time as applicable regulations are amended or clarified. Institutions may however, find it useful to apply the concepts underlying the examples in this guidance to their own electronic financial service operations. The electronic financial services environment is dynamic thus, the guidance outlined in this letter could also evolve based on developments in technology and the continuation of deliberations regarding appropriate policies.

ADVERTISEMENTS

Generally, Internet web sites are considered advertising by the regulatory agencies. In some cases, the regulations contain special rules for multiple-page advertisements. It is not yet clear what would constitute a single "page" in the context of the Internet or on-line text. Thus, institutions should carefully review their on-line advertisements in an effort to minimize compliance risk.

In addition, Internet or other systems in which a credit application can be made on-line may be considered "places of business" under HUD's rules prescribing lobby notices. Thus, institutions may want to consider including the "lobby notice," particularly in the case of interactive systems that accept applications.

DISCLOSURES/NOTICES

Several consumer regulations provide for disclosures and/or notices to consumers. The compliance officer should check the specific regulations to determine whether the disclosures/notices can be delivered via electronic means. The delivery of disclosures via electronic means has raised many issues with respect to the format of the disclosures, the manner of delivery, and the ability to ensure receipt by the appropriate person(s). The following highlights some of those issues and offers guidance and examples that may be of use to institutions in developing their electronic services.

Disclosures are generally required to be "clear and conspicuous." Therefore, compliance officers should review the web site to determine whether the disclosures have been designed to meet this standard. Institutions may find that the format(s) previously used for providing paper disclosures may need to be redesigned for an electronic medium. Institutions may find it helpful to use "pointers[1]" and "hotlink[2]" that will automatically present the disclosures to customers when selected. A financial institution's use solely of asterisks or other symbols as pointers or hotlinks would not be as clear as descriptive references that specifically indicate the content of the linked material.

Several regulations also require disclosures and notices to be given at specified times during a financial transaction. For example, some regulations require that disclosures be given at the time an application form is provided to the consumer. In this situation, institutions will want to ensure that disclosures are given to the consumer along with any application form. Institutions may accomplish this through various means, one of which may be through the automatic presentation of disclosures with the application form.

Regulations that allow disclosures/notices to be delivered electronically and require institutions to deliver disclosures in a form the customer can keep have been the subject of questions regarding how institutions can ensure that the consumer can "keep" the disclosure. A consumer using certain electronic devices, such as Web TV, may not be able to print or download the disclosure. If feasible, a financial institution may wish to include in its on-line program the ability for consumers to give the financial institution a non-electronic address to which the disclosures can be mailed.

In those instances where an electronic form of communication is permissible by regulation, to reduce compliance risk institutions should ensure that the consumer has agreed to receive disclosures and notices through electronic means. Additionally, institutions may want to provide information to consumers about the ability to discontinue receiving disclosures through electronic means, and to implement procedures to carry out consumer requests to change the method of delivery.

Furthermore, financial institutions advertising or selling non-deposit investment products through on-line systems, like the Internet, should ensure that consumers are informed of the risks associated with nondeposit investment products as discussed in the "Interagency Statement on

[1] A "pointer" is a declarative statement that refers to the location within the system at which additional important information begins.

[2] A "hotlink" is an electronic connection between two or more electronic documents that are not in sequential order.

Retail Sales of Non Deposit Investment Products." On-line systems should comply with this Interagency Statement, minimizing the possibility of customer confusion and preventing any inaccurate or misleading impression about the nature of the nondeposit investment product or its lack of FDIC insurance.

ELECTRONIC STORED VALUE PRODUCTS

Electronic stored value products are retail payment products in which value is recorded on a personal electronic device or on a magnetic strip or computer chip in exchange for a predetermined balance of funds. Electronic stored value products may include stored value cards, smart cards, and electronic cash recorded on a personal electronic device, such as a personal computer. Electronic stored value cards can be either disposable or reloadable. Disposable cards are purchased with a specific electronic value embedded on the card that can be used for transactions until the electronic value is depleted. A reloadable card permits a user to increase, as necessary, the value on the card at an electronic terminal or device that accepts currency or that allows the user to transfer funds from an account to the card.

The Federal Reserve Board of Governors, in its Report to the Congress on the Application of the Electronic Fund Transfer Act to Electronic Stored-Value Products, for purposes of the study, describes electronic stored value products as retail payment products intended primarily for consumer payments that generally have some or all of the following characteristics:

- A card or other device that electronically stores or provides access to a specified amount of funds selected by the holder of the device and available for making payments to others.
- The device is the only means of routine access to the funds.
- The issuer does not record the funds associated with the device as an account in thename of (or credited to) the holder.

The application of certain consumer protection laws and regulations to these products has not been determined. However, financial institutions that issue electronic stored value products may wish to provide information to consumers about the operation of these products to enable consumers to meaningfully distinguish among different payment products, such as stored value cards, debit cards and credit cards. Additionally, consumers likely would find it beneficial to receive information about the terms and conditions associated with the use of electronic stored value products, to ensure their informed use of these products. Some financial institutions that issue stored value products have provided consumers with a variety of disclosures including:

- federally insured or non-insured status of the product,
- all fees and charges associated with the purchase, use or redemption of the product,
- a any liability for lost or stolen electronic stored value,
- any expiration dates, or limits on redemption of the electronic stored value, and
- toll-free telephone number for customer service, malfunction and error resolution.

FDIC General Counsel Opinion No. 8, dated July 16, 1996, states that insured depository institutions are expected to disclose in a clear and conspicuous manner to consumers the insured or non-insured status of the stored value products they offer to the public, as appropriate. Some

financial institutions have also printed some of this information, such as expiration date and telephone number, directly on the card.

Financial institutions should also consider establishing procedures to resolve disputes arising from the use of the electronic stored value products.

Record Retention

Record retention provisions apply to electronic delivery of disclosures to the same extent required for non-electronic delivery of information. For example, if the web site contains an advertisement, the same record retention provisions that apply to paper-based or other types of advertisements apply. Copies of such advertisements should be retained for the time period set out in the relevant regulation. Retention of electronic copies is acceptable.

THE ROLE OF CONSUMER COMPLIANCE IN DEVELOPING AND IMPLEMENTING ELECTRONIC SERVICES

When violations of the consumer protection laws regarding a financial institution's electronic services have been cited, generally the compliance officer has not been involved in the development and implementation of the electronic services. Therefore, it is suggested that management and system designers consult with the compliance officer during the development and implementation stages in order to minimize compliance risk. The compliance officer should ensure that the proper controls are incorporated into the system so that all relevant compliance issues are fully addressed. This level of involvement will help decrease an institution's compliance risk and may prevent the need to delay deployment or redesign programs that do not meet regulatory requirements.

The compliance officer should develop a compliance risk profile as a component of the institution's online banking business and/or technology plan. This profile will establish a framework from which the compliance officer and technology staff can discuss specific technical elements that should be incorporated into the system to ensure that the online system meets regulatory requirements. For example, the compliance officer may communicate with the technology staff about whether compliance disclosures/notices on a web site should be indicated or delivered by the use of "pointers" or "hotlinks" to ensure that required disclosures are presented to the consumer. The compliance officer can also be an ongoing resource to test the system for regulatory compliance.

Compliance officers will need to review their existing compliance policies and procedures and make appropriate modifications based upon the types of products, services, and operating features of the institution's online system. The compliance program may not need to be revamped, but merely extended to address the new level of technology employed by the institution. Staff should be trained and a monitoring system implemented to review continually the content and operation of the online programs to prevent inadvertent or unauthorized changes that may affect compliance with the regulations.

Management should review and revise the institution's electronic financial services as the regulatory environment changes and electronic delivery mechanisms evolve. This will help to ensure that the institution maintains an effective compliance program.

CONCLUSION

This guidance provides information for institutions to consider during the design, development, implementation and monitoring of electronic banking operations. Financial institutions are responsible for ensuring that their electronic banking operations are in compliance with applicable laws, regulations, and policies, including both federal and state provisions.

Financial institutions need to adapt to a changing technological environment so that compliance with consumer protections laws are maintained, while allowing the financial institution industry to continue to make effective use of new technology. Due to the continuing evolution of the technological environment and the associated regulatory environment, proposed changes to federal laws and regulations will undoubtedly affect the content of this letter in the future. The regulatory agencies are interested and willing to discuss these issues with financial institutions during the design and development of their electronic banking programs. Additionally, regulatory agency Internet sites may also contain information helpful to financial institutions.

Interagency Guidance on Electronic Financial Services and Consumer Compliance

ON-LINE SERVICES: INTERNET, PERSONAL COMPUTER, INTERACTIVE TELEVISION OR VIDEO KIOSKS, ETC.

Advertising and Information Only Systems

Includes advertising of loans, leases. deposit services - Truth in Lending Act, Equal Credit Opportunity Act, Consumer Leasing Act, Truth in Savings Act and Fair Housing Act apply.

- Unfair or Deceptive Advertising -- Consider state laws that may apply
- FDIC official advertising statement and Equal Housing Lending logo
- Information displayed as a on-line "lobby board" or scrolling message may constitute an advertisement

On-line Depository Services

Electronic Fund Transfer Act, Expedited Funds Availability Act, Truth in Savings Act, and Regulation D (Reserve Requirements Depository Institutions) apply.

- Major areas for consideration: delivery of disclosures; notices; periodic statements; error resolution procedures
- Ensure appropriate account authorization, including signature issues
- Determine appropriate manner of delivering written notices and/or other information to and from the customer with an on-line account
- Ensure disclosures are delivered in a timely manner and are "clear and conspicuous" / "clear and readily understandable" as required
- Ensure that correspondence and requests for information received from consumers via on-line or electronic communication are responded to in accordance with the regulations
- Consider BSA "Know your customer implications

Lending and Leasing Services

Equal Credit Opportunity Act, Home Mortgage Disclosure Act, Consumer Leasing Act, Truth in Lending Act, Unfair and Deceptive Practices Act, Community Reinvestment Act, Fair Credit Reporting Act, and the Fair Housing Act apply.

- Major areas for consideration: delivery of disclosures; notices; periodic statements; error resolution procedures
- Determine appropriate manner of delivering "written" notices and/or other information to and from the customer with an on-line account
- Ensure disclosures are delivered in a timely manner and are "clear and conspicuous" standard as required
- Ensure timely delivery of Adverse Action Notices in an appropriate manner
- Ensure that on-line products are offered and evaluated on a nondiscriminatory basis and that no illegal discouragement exists
- Determine that monitoring information and/or data collection requirements of Regulation B, C, and BB are handled appropriately
- Ensure that applications taken on-line receive the information required by the regulation
- Ensure that correspondence received from consumers via electronic communication are responded to in accordance with the regulations

Non-Deposit Investment Products

Includes securities, mutual funds, and annuities
See Interagency Statement on Retail Sales of Non-deposit Investment Products.

- Ensure appropriate notices are provided or posted indicating the services are not FDIC-insured, not guaranteed by the bank, and subject to loss of principal
- Consider whether non-deposit investment sales are appropriately segregated from where retail deposits are solicited in an on-line environment

Office of Thrift Supervision

Policy Statement on Privacy and Accuracy of Personal Customer Information
November 1998

INTRODUCTION

Savings associations regulated by the Office of Thrift Supervision ("OTS") have an obligation to protect and maintain confidential and accurate customer information. Institutions have already established internal controls to protect paper-based personal information. Institutions are now, however, faced with new challenges presented by the electronic storage and retrieval of information. As financial institutions increasingly use new technology to access, compile, and relay information to the customer, other institution staff, and third parties, new concerns arise about the privacy, security, and accuracy of such data. New technology also increases the potential for misuse or alteration of information.

This policy statement recommends that savings associations ("you") notify customers how you will use certain customer information and permit them to limit your use of it. It also reminds you to establish adequate controls to protect and maintain the confidentiality and accuracy of all customer information. Your written procedures should:

- Inform customers how you will use certain customer information and permit customers to limit the use of such information; and
- Safeguard the security and accuracy of all information about customers.

RECOMMENDED PRACTICES TO INFORM CUSTOMERS AND OBTAIN CONSENT FOR THE USE OF PERSONAL INFORMATION[1]

Before you collect any information from a customer, you should describe to that customer how you will use his or her personal information. For example, you may initially need specific information to open an account or authorize a loan for the customer. However, you may also want to share that personal information with your affiliates to cross-market other products or services to the customer.

There are many ways for you to provide adequate notice to your customers about use of their personal information. For example, when you open an account with a customer, you should consider providing the customer a notice that explains:

[1] The term "personal information," as used in this policy statement, does not include "information solely as to transactions or experiences between the customer and the [institution]" as provided in the Fair Credit Reporting Act, 15 U.S.C. § 1681a(d)(2)(A)(i).

- all intended uses of the personal information you are collecting;
- whether you intend to give or sell the personal information to an affiliated or non-affiliated party;
- what happens if the customer declines to provide the required information;
- a general description of the methods you use to assure the confidentiality and accuracy of information; and
- a phone number, e-mail address, or other point of contact at your institution that the customer can use to:
  - ⇒ review information that you have about the customer;
  - ⇒ correct inaccurate or outdated information; or
  - ⇒ notify you of possible unauthorized access to, or use of, his or her account information.

Existing customers and the general public may also want to read your customer notice. You may want to make this notice available upon request.

Before sharing personal information with affiliates, the Fair Credit Reporting Act requires that you disclose to the customer that you may share the information with affiliates and give the customer the opportunity to "opt out" of having this information shared with affiliates. We also recommend you offer your customers the choice to opt out of having this information shared with non-affiliated parties. Furthermore, certain federal and state privacy laws prohibit the release of a customer's financial records without the customer's permission.[2] If the customer has chosen to limit your sharing of their personal information, you may not exchange or sell personal information about the customer to third parties, unless you:

- receive a customer request or permission to release the information; or
- are required or allowed by law (e.g., subpoena or investigation of fraud) to disclose the information.

If you provide personal customer information to a service provider or other reporting agency under an outsourcing arrangement you should assure that they continue to protect the security and accuracy of such information.

[2] The federal Right to Financial Privacy Act ("RFPA"),, prohibits the release of the financial records of any custmer to any "Government authority" except in accordance with the requirements of the RFPA. 12 U.S.C. § 3403. For a listing of other privacy laws, *see* Federal Trade Commission, Privacy Online: A Report to Congress 40, n.160 (June 1988) and "The Report of the Consumer Electronic Payments Task Force" 24-29 (April 1998).

SAFETY AND SOUNDNESS STANDARD TO KEEP INFORMATION SECURE AND ACCURATE

Institutions already have internal controls in place that address the security of paper-based information. Specifically, you should have procedures for access, storage, and disposal of documents that contain confidential customer information.

In addition to handling paper documents within traditional brick and mortar facilities, financial institutions may use delivery channels (e.g., public telephone networks and the Internet) that are partially or totally outside the control of the institution. Operational risks increase with the reach of systems and the number of uncontrolled access points to the information.[3] Access to your electronic records through a local network, telephone or the Internet could potentially open your computer system to unauthorized users.[4] Therefore, adequate security of your institution's systems and customer information is paramount. Your internal controls must be updated to reflect the use of developing technologies and continue to adequately safeguard customer information. You should ensure that all employees are aware of their responsibilities to safeguard customer information. A comprehensive security program:

- Establishes controls to guard against unauthorized access to your networks, systems, and databases;
- Provides for employee training;
- Protects customers during transmissions over public networks to ensure the intended person receives accurate information and to prevent eavesdropping by others;
- Creates proof that both the sender and the receiver participated in a transaction: it is important that you ensure neither party in a transaction can deny his or her obligation;[5]
- Ensures the integrity and accuracy of your customer account information;
- Provides for correcting or updating information that you still use in account data files; and,
- Permits customers to review and correct any erroneous or outdated information.

If you collect, process, or maintain customer financial information, you should perform certain

[3] Operational risks arise from the potential that breaches of internal controls, operating problems, fraud, inadequate information systems, or unforeseen events may result in unexpected losses.

[4] For instance, "information brokers," operating generally over the telephone and the Internet, can obtain detailed information about a customer's financial history from financial institutions. You need to ensure that confidential customer account information is not inappropriately provided to information brokers. (For additional guidance on "information brokers," you can refer to the "Interagency Pretext Phone Calling Memorandum.") Also, outside hackers, disgruntled employees, unauthorized internal users and others may create havoc with your customer information if you fail to establish adequate operating controls.

[5] The *OTS Thrift Activities Handbook*, Section 341, Information Technology offers specific guidance on the type of controls that management should implement to ensure adequate security of information and authentication of users.

functions (e.g., account balance reconciling, funds transfer, or bill payments) under dual control. You should segregate the input of information from the review of processed information. These controls should also require the reviewer to reconcile the processed information. Your operating policies and procedures should describe the appropriate controls in detail.

SUMMARY

You should have written policies and procedures, approved by your board of directors, that describe how you will ensure that information is properly protected, confidential, and used as agreed with the customer. This policy statement and applicable laws and regulations will be considered by OTS examiners as they evaluate the adequacy of your internal controls.

OTHER SOURCES OF INFORMATION

Other federal agencies and bank industry trade groups also have issued privacy guidance that you may find useful. This includes:

- *"Privacy Online: A Report to Congress,"* Federal Trade Commission June 1998. (A description of core principles of fair information practices.) This report can be found on the Federal Trade Commission's web site at www.ftc.gov.

- *"Online Privacy of Consumer Personal Information,"* Federal Deposit Insurance Corporation August 1998. (A financial institutions letter that addresses online privacy to raise awareness among financial institutions.) This report can be found on the Federal Deposit Insurance Corporation's web site at www.fdic.gov.

- *"Emerging Privacy Issues in Electronic Banking,"* America's Community Bankers August 1998. (A description of specific operating privacy principles for community banks.) This report can be found on the trade association's web site at www.acbankers.org.

- *Banking Industry Privacy Principles," American* Bankers Association, Consumer Bankers Association, and the Bankers Roundtable. (Joint industry privacy principles for the benefit of bankers and consumers.) This report can be found on several trade associations' web sites such as www.aba.com or www.cbanet.org.

Office of Thrift Supervision

Interagency Pretext Phone Calling Memorandum
November 1998

PURPOSE

This memorandum alerts insured financial institutions to the practice of "pretext phone calling," which is a means of gaining access to customers' confidential account information by organizations and individuals who call themselves "account information brokers." It is intended to enhance institutions' awareness regarding the confidentiality and sensitivity of customer information generally, and identify some appropriate measures for the safeguarding of such information.

This guidance was jointly prepared by the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the Federal Reserve Board, the FBI, the Secret Service, the Internal Revenue Service, and the Postal Inspection Service.

BACKGROUND

There is a tremendous demand for information about individuals' and businesses' bank accounts. In recent years, this rising demand for account information has led to an increase in the number of organizations known as "account information brokers." These "brokers" gather confidential financial information, including specific account numbers and balances, from various public and nonpublic sources. The brokers then sell this information to anyone who is willing to pay for it. Their clients include lawyers, debt collection services, and private investigators, who may use account information in civil lawsuits and other court proceedings, or identity thieves who may use account information to engage in check and credit card fraud, and other criminal acts.

Unscrupulous account information brokers are obtaining customers' account information from insured financial institutions through a practice known as "pretext phone calling" or "social engineering." Brokers who engage in this practice call institutions and use surreptitious or fraudulent means to try to induce employees into providing a customer's account information. For example, a broker may pose as a customer who has misplaced his or her account number, and may repeatedly call the institution until the broker finds an employee who is willing to divulge confidential account information. The broker may use information about the customer, such as the customer's social security number, that has been obtained from other sources, to convince the employee that the caller is legitimate. While there are no reliable estimates as to the extent of this practice, there is concern among the federal banking and law enforcement agencies that it is becoming increasingly prevalent.

The use of surreptitious or fraudulent means to obtain a customer's account information may violate state and federal laws prohibiting unfair and/or deceptive practices. It also may violate federal wire fraud laws. In addition, institutions that disclose customers' account information may be violating state privacy laws, such as those that prohibit the release of a customer's financial records without having first obtained the customer's permission.

RECOMMENDED ACTIONS

Institutions have an obligation to their customers to ensure that their customers' account information is not improperly disclosed. Authorizing employees to use their own discretion to determine whether to disclose confidential information over the telephone can result in inconsistent practice and expose the institution and its customers to the risk of an inappropriate or unauthorized release of information. To avoid this risk, institutions are encouraged to develop policies and procedures for addressing customers' financial privacy, and should, at a minimum, establish clear guidelines for dissemination of customer account information. These guidelines should set forth precisely the types of information and the circumstances under which an employee is allowed to disseminate such information over the telephone. Employee training should ensure that all employees are aware of their responsibility to safeguard customer financial information, and also should educate employees of the tactics used by information brokers to surreptitiously or fraudulently obtain confidential customer information.

Institutions should have strong controls in place to ensure against the unauthorized disclosure of customer information. For example, they should consider adopting a policy that prohibits the release of information over the telephone unless the proper authorization code is provided. The authorization code should be used in the same manner as a personal identification number (PIN) for transacting business by automatic teller machines, or credit, debit, or stored-value cards. The authorization code should not be associated with other commonly used numbers or identifiers, such as social security numbers, savings, checking, loan or other financial account numbers, PINS, or the customer's mother's maiden name. In addition, the authorization code should be unique to, and readily changed by, the authorized account holder. Finally, to increase effectiveness, the authorization code should be used in conjunction with other customer and account identifiers.

Another means of preventing unauthorized disclosures is to use a caller identification service or require employees who receive calls requesting account information to ask the caller for the number from which he or she is calling. If the number differs from that in the customer's account records, it may be an indication that the request is not a legitimate one, and the employee should not disclose the requested account information without taking further steps to verify that the customer made the request.

The institution's security or internal audit department should consider conducting (or using third parties to conduct) unscheduled pretext phone calls to various departments to evaluate the institution's susceptibility to unauthorized disclosures of customer information. Any weaknesses detected should be addressed through the adoption of enhanced training, procedures, and controls.

While this memorandum primarily concerns the unauthorized access to customer account information through pretext phone calling, unauthorized access to sensitive account information may occur through other means as well, including burglary, illegal or unauthorized access to the institution's computer systems, and bribing employees with access to personal account information. Institutions should have effective procedures and controls in place to limit access to confidential information on a need to know basis, and to prevent unauthorized access to customer information through these and other means, including ensuring that all sensitive documents are properly disposed of and that the institution's physical premises and computer systems are secure. Institutions also must properly train employees to understand the importance of protecting personal account information against improper disclosure. The federal banking agencies will continue to monitor institutions' efforts to safeguard sensitive account information.

Institutions that suspect an illicit attempt to obtain a customer's confidential information should immediately report the matter to the proper authorities. In such circumstances, institutions are encouraged to file a Suspicious Activity Report, and to contact their primary federal banking regulator, the Federal Trade Commission, and the appropriate state agencies charged with enforcing laws against unfair or deceptive practices. In addition, institutions should directly contact appropriate law enforcement agencies if a fraud requiring immediate attention is suspected.

Children's Online Privacy Protection Act

Background and Summary

The Children's Online Privacy Protection Act of 1998 (COPPA) (15 USC 6501 et seq.) addresses the collection, use, or disclosure of personal information about children that is collected from children through websites or other online services. On November 3, 1999, the Federal Trade Commission (FTC) issued a regulation (16 CFR 312), which implements COPPA. The regulation became effective on April 21, 2000.

Financial institutions are subject to COPPA if they operate a website(s) or online service(s) (or portion thereof) directed to children, or have actual knowledge that they are collecting or maintaining personal information from a child online. COPPA grants each of the federal financial regulatory agencies enforcement authority over the institutions they supervise under 12 USC 1818.

Definitions

The terms "child" or "children" mean individuals under the age of 13.

The term "personal information" means individually identifiable information about an individual collected online, including first and last name, home address, e-mail address, telephone number, social security number, or any combination of information that permits physical or online contact.

COPPA employs several other definitions including "communication," "disclosure" and "verifiable parental consent." For the complete listing of definitions see 16 CFR 312.2.

The following examination procedures should be consulted when examining an institution for whom any part of the company's website is directed to or captures information from children. At the close of the exam procedures, you will find the General Requirements of the COPPA regulation as well as a brief synopsis of the specific regulatory sections (e.g. Content, Notice to a Parent, Placement of Notice on website). Finally, the last document in this section is a COPPA Worksheet, a numbered checklist, to be used at the close of this particular section of the examination.

Initial Procedures

1. From direct observation of the institution's website or online service and through discussions with appropriate management officials, ascertain whether the financial institution is subject to COPPA by determining if it operates a website(s) or online service(s) that:

   - Is directed to children; or

   - Knowingly collects or maintains personal information from children. A thrift knowingly collects or maintains information from a child when it requests age or birth date information on its website and persons under age 13 can and do respond by providing age or birth date combined with other individually identifiable information.

   If the institution does <u>not</u> currently operate a website directed to children or knowingly collects information about them, the institution <u>is not</u> subject to COPPA and no further examination procedures are necessary.

2. If the institution is subject to COPPA, determine if it is participating in an FTC-approved self-regulatory program. If yes, obtain a copy of the program, and supporting documentation, such as reviews or audits, which demonstrate the institution's compliance with the program. If the self-regulatory authority (SRA) determined that the institution was in compliance with COPPA at the most recent review/audit, or has not yet made a determination, no further examination procedures are necessary. If however, the SRA determined that the institution was not in compliance with COPPA and the institution has not taken appropriate corrective action, complete the remaining procedures.
3. If an institution is subject to COPPA, review applicable audit and compliance program materials to determine whether:

   - Internal review procedures address the COPPA provisions applicable to the institution;
   - The audits or reviews performed were reasonable, accurate and include consideration of issues raised by consumer complaints;
   - Effective corrective action occurred in response to previously identified deficiencies;
   - Deficiencies, their causes, and the effective corrective actions are consistently reported to management or the members of the board of directors; and
   - The frequency of compliance review is appropriate for the level of changes to on-line content.

4. If an institution is subject to COPPA, but does not conduct satisfactory internal audits or compliance reviews, evaluate whether the institution's internal controls are adequate to ensure compliance with COPPA. Consider:

   - Who in the organization is responsible for the institution's compliance with COPPA;
   - Process flowcharts to determine how the institution's COPPAA compliance is planned for, evaluated, and achieved;
   - Policies, procedures and training programs;
   - How methods of collecting or maintaining personal information from the website or online service are vetted before implementation;
   - How data elements collected from a child are tracked for use and protected;
   - Whether data elements collected from a child are disclosed to third parties and how permission for such disclosure is implemented and tracked;
   - The resolution process for complaints regarding the treatment of data collected from a child; and
   - Any system triggers to alert operations staff about potential COPPA ramifications of web content decisions.

5. Based on the results of the foregoing, determine which verification procedures, if any, should be completed, focusing on the areas of particular risk. The selection of procedures to be employed depends upon the adequacy of the institution's compliance management system and level of risk identified. It may be most efficient to have management conduct any necessary review, correct any self-identified deficiencies and report to the Region a self-assessment of its COPPA compliance.

Verification Procedures

1. Through testing or management's demonstration of the website or online service, verify that the financial institution does not condition a child's participation in a game, offering of a prize, or another activity on the child's disclosure of more personal information than is reasonably necessary to participate in the activity [16 CFR 312.7].
2. Obtain a sample of data collected on children including data shared with third parties, if applicable, and determine whether:

   - The financial institution has established and maintained reasonable procedures to protect the confidentiality, security and integrity of personal information collected from a child [16 CFR 312.8 and 312.3];
   - Data are collected, used, and shared in accordance with the institution's website notice [16 CFR 312.4 and 312.3]; and
   - Parental permission was obtained prior to the use, collection or sharing of information, including consent to any material change in such practices [16 CFR 312.5(a)].

3. Through testing or management's demonstration of the website or online service and a review of a sample of parental consent forms or other documentation determine whether the financial institution has a reasonable method for verifying the person providing the consent is the child's parent [16 CFR 312.5 (b)(2)].
4. Review a sample of parent requests for personal information provided by their children and verify that the financial institution:

   - Provided, upon request, a description of the specific types of personal information collected [16 CFR 312.6(a)(1)];
   - Complied with a parent's instructions concerning the collection or disclosure of their child's information. [16 CFR 312.6(a)(2)];
   - Allowed parents to review any personal information collected from the child [16 CFR 312.6(a)(3)]; and
   - Verified that persons requesting information are parents of the child [16 CFR 312.6 (a)(3)].

5. Complete the COPPA Worksheet on access, clarity and content of electronic notices on the thrift's website or online service. (see "Attachment A").

Conclusions

1. Summarize all findings, supervisory concerns and regulatory violations.
2. For the violation(s) above, determine the root cause by identifying weaknesses in internal controls, audit and compliance reviews, training, management oversight, or other factors; also, determine whether the violation(s) are repetitive or systemic.
3. Identify action needed to correct violations and weaknesses in the institution's compliance system.
4. Discuss findings with the institution's management and obtain a commitment for corrective action.

General Requirements of the COPPA Regulations

The regulation requires an operator of a website or online service directed to a child, or any operators who have actual knowledge that they are collecting or maintaining personal information from a child, to:

- Provide a clear, complete and understandably written notice on the website or online service of their information collection practices with regard to children, describing how the operator collects, uses and discloses the information (16 CFR 312.4);
- Obtain, through reasonable efforts and with limited exceptions, verifiable parental consent prior to the collection, use or disclosure of personal information from children (16 CFR 312.5);
- Provide a parent, upon request, with the means to review the personal information collected from his/her child and to refuse to permit its further use or maintenance (16 CFR 312.6);
- Limit collection of personal information for a child's online participation in a game, prize offer, or other activity to information that is reasonably necessary for the activity (16 CFR 312.7); and
- Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal information collected from children (16 CFR 312.8).

Placement of Notice on the Website [16 CFR 312.4(b)(1)]

An operator of a website or online service directed to children must post a link to a statement describing how it collects, uses and discloses information from and about any child on its homepage and everywhere on the site or service where it collects personal information from any child. An operator of a general audience website that has a separate children's area must post a link on the home page of the children's area.

These links must be placed in a clear and prominent place on the home page of the website or online service. To make a link clear and prominent, a financial institution may, for example, use a larger font size in a different color on a contrasting background. A link in small print at the bottom of a home page does not satisfy the clear and prominent guidelines.

Content [16 CFR 312.4(b)(2)]

The notice must state among other requirements:

- The name, address, telephone number and e-mail address of all operators collecting or maintaining personal information from any children through the website or online service;
- The types of personal information collected from any children and how the information is collected;
- How the operator uses the personal information;
- Whether the operator discloses information collected to third parties. If it does, the notice must state the types of businesses engaged in by the third parties, the purposes for which the information is used, and whether the third parties have agreed to maintain the confidentiality, security and integrity of the information. In addition, the notice must state that the parent has the option to consent to the collection and use of the information without consenting to the disclosure of the information to third parties;
- That the operator may not require as a condition of participation in an activity that a child disclose more information than is reasonably necessary to participate in such activity; and

- That a parent can review his or her child's personal information, have it deleted, and refuse to allow any further collection or use of the child's information, and state the procedures for doing so.

Notice to a Parent [16 CFR 312.4 (c)]

An operator is required to obtain verifiable parental consent before any collection, use or disclosure of personal information from any children. An operator also must make reasonable efforts to provide a parent with notice of the operator's information practices with regard to children, as described above, and in the case of a notice seeking consent, the following additional information:

- The operator wishes to collect personal information from the parent's child;
- The parent's consent is required for the collection, use and disclosure of the information; and
- How the parent can provide consent.

Methods for Obtaining Parental Consent [16 CFR 312.5 (b)]

Until April 2002, the FTC will use a sliding scale approach for obtaining parental consent in which the required method of consent will vary based on how the financial institution intends to use the child's personal information. If the information is used for internal purposes, which may include an operating subsidiary or affiliate, a less rigorous method of consent is required. If the financial institution discloses the information to others, the child's privacy is at greater risk, and a more reliable method of consent is required. Anticipating that technical developments soon will allow companies to use more reliable methods to verify identities, the FTC expects to phase out the sliding scale approach by April 2002, subject to an FTC review planned for October, 2001.

Internal Uses

Financial institutions that use the personal information internally may use e-mail to get parental consent provided the operator takes additional steps to verify that a parent is the person providing consent, such as by confirming receipt of consent by e-mail, letter, or telephone call.

Disclosure to Others

Disclosure of a child's personal information to others (e.g., chat rooms, message boards, and third parties) presents greater risk to a child's privacy, and the FTC's sliding scale approach noted above, requires a more reliable method of consent, including:

- Obtaining a signed consent form from a parent via postal mail or facsimile;
- Accepting and verifying a credit card number;
- Taking a parent call, through a toll-free telephone number staffed by trained personnel;
- E-mail accompanied by digital signature; or
- E-mail accompanied by a PIN or password obtained through one of the methods mentioned above.

Disclosures to Third Parties

A parent may permit an operator of a website or online service to collect and use information about a child while prohibiting the operator from disclosing the child's information to third parties. An operator must give a parent this option.

Parental Consent to Material Changes [16 CFR 312.5(a)]

The operator must send a new notice and request for consent to a parent if there are material changes in the collection, use or disclosure practices to which a parent has previously agreed.

Exceptions to Prior Parental Consent Requirement [16 CFR 312.5(c)]

A financial institution does not need prior parental consent when it is collecting:

- A parent's or child's name or online contact information solely to obtain consent or to provide notice. If the operator has not obtained parental consent after a reasonable time from the date of the information collection, the operator must delete such information from its records;
- A child's online contact information solely to respond on a one-time basis to a specific request from the child, if the information is not used to recontact the child, and is deleted by the operator;
- A child's e-mail address to respond more than once to a specific request of the child (e.g., a request to receive a monthly online newsletter), when the operator does not use the information to contact the child beyond the scope of the request, and a parent is notified and allowed to request that the information not be used further;
- The name and online contact information of the child to be used solely to protect the child's safety; or
- The name and online contact information of the child solely to protect the security of the site, to take precautions against liability, or to respond to judicial process, law enforcement agencies, or an investigation related to public safety.

Right to Review Information [16 CFR 312.6]

An operator of a website or online service is required to provide a parent with a means to obtain any personal information collected from his or her child. At a parent's request, an operator must provide a parent with:

- A description of the types of personal information it has collected from the child; and
- An opportunity to review the information collected from the child.

Before a parent can review a child's information, the operator must take steps to ensure that the person making the request is the child's parent. An operator or its agent will not be held liable under any federal or state laws for any disclosures made in good faith and following reasonable procedures to verify a requester's identity in responding to a request for disclosure of personal information.

The regulations allow parents to refuse to permit an operator to continue to use or to collect their child's personal information in the future and to instruct the operator to delete the information. If a parent does so, an operator may terminate its service to that child.

Confidentiality, Security and Integrity of Personal Information Collected from a Child [16 CFR 312.8]

The operator of a website or an online service is required to establish and maintain reasonable procedures to protect the confidentiality, security and integrity of personal information collected from any children. Operators must have adequate policies and procedures for protecting a child's personal information from loss, misuse, unauthorized access or disclosure. Operators are allowed to select an appropriate method for implementing this provision.

Safe-harbor [16 CFR 312.10]

Industry groups, financial institutions or others may establish, with the FTC's approval, a self-regulatory program. An operator of a website or online service that complies with FTC-approved self-regulatory guidelines will receive a "safe harbor" from the requirements of COPPA and the regulations. Self-regulatory guidelines must require that a website and an online service implement substantially similar requirements that provide the same or greater protections for a child as the FTC regulations (16 CFR 312.2-9). These guidelines also must include an effective, mandatory mechanism for assessing operators' compliance, as well as incentives to ensure that an operator will comply.

This page intentionally left blank

Attachment A

Children's Online Privacy Protection Act Worksheet for Notices

Website Notice (16 CFR 312.4)	Yes	No
1. A link is posted on the website to a notice of the financial institution's information practices with regard to children. [16 CFR 312.4 (b)].		
2. The link to the notice is clearly labeled as a notice of the website's information practices with regard to children, and is placed in a clear and prominent place on the home page of the website and at each area on the website where a child directly provides personal information [16 CFR 312.4(b)(1)].		
3. The notice states:		
• The name, address, telephone number, and e-mail address of any operator who collects or maintains personal information from a child through the website [16 CFR 312.4(b)(2)(i)];		
• The types of information collected from a child and whether the information is collected directly or passively [16 CFR 312.4(b)(2)(ii)];		
• How such information is or may be used [16 CFR 312.4(b)(2)(iii)];		
• Whether such information is disclosed to a third party and, if so, determine whether:		
- The notice states the types of businesses engaged in by the third parties;		
- The purposes for which the information is used;		
- The third parties have agreed to maintain the confidentiality, security and integrity of the information; and		
- That a parent has the option to consent to the collection and use of the information without consenting to the disclosure; [16 CFR 312.4(b)(2)(iv)];		
• The operator is prohibited from conditioning a child's participation in an activity on the disclosure of more information than is reasonably necessary to participate in such activity [16 CFR 312.4(b)(2)(v)]; and		
• A parent can review and have deleted the child's personal information; and		
- Refuse to permit further collection or use of the child's information; and		
- States the procedures for doing so [16 CFR 312.4(b)(2)(vi)].		

	Yes	No
4. The notice to a parent		
• States that the operator wishes to collect information from the child.		
• Includes the information contained in the §312.4(b) website notice (see step 3 above) [16 CFR 312.4(c)(1)(i).		
• If §312.5(a) applies, states that the parent's consent is required for the collection, use and/or disclosure of such information and states the means by which the parent can provide verifiable consent to the collection of information. [16 CFR 312.4(c)(1)(ii).		
• Includes additional information as detailed in the regulation if the exceptions in §312.5(c)(3) and (4) apply.		